

### REMARKS

The examiner rejected Claims 3, 4, 9, 15-17, 21, and 24 under 35 U.S.C. 112, second paragraph, as being indefinite.

Applicant has amended claims 3 and 24 to provide antecedent basis for "overview page."

Claim 9 has been amended to provide antecedent basis for "host attempted to connect to."

Claim 15 has been amended to "historically normal operating conditions." The term "normal" is to referenced to an historical norm, and therefore, the metes and bounds of the claim are definite.

Claim 21, has been amended to recite: "... claim 20 wherein the network statistics are a number of bytes ... ." Antecedent basis has been provided for this term in the claim and the claim is therefore definite.

### 35 U.S.C § 103

The examiner rejected claims 1-9 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper US Patent Application Publication 2002/0069200 (hereinafter Cooper), and in view of Symantec's Symantec Antivirus for Macintosh SAM, 1994, (hereinafter Symantec).

### Claim 1

In rejection of claim 1, the examiner argued:

As per claim 1, Cooper teaches a graphical user interface for an intrusion detection system, the graphical user interface comprising: a field that depicts a summary of anomalies identified as part of a event that is detected in a network (throughout the reference, such as Figure 26, paragraph 514, abstract, paragraph 42), the summary indicating event severity details of the event (Figure 26). However, at the time of the invention. Cooper does not explicitly teach an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time. A snooze for future alerts is taught Symantec though, such as in pages 4-9 and 5-6, wherein an event may be allowed to continue, and an alert may be prevented from appearing in the future.

At the time of the invention, it would have been obvious to combine the teachings of Cooper with Symantec. One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user.

**Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity.**

Claim 1 is directed to graphical user interface rendered on a display associated with an intrusion detection system. Inventive features of claim 1 include a field that depicts a summary of anomalies identified as part of an event ... detected in a network, the summary indicating event severity ... and ... a control to permit a user to snooze future alerts related to the event in the summary for a period of time.

The examiner argues that “Cooper teaches a graphical user interface for an intrusion detection system, the graphical user interface comprising: a field that depicts a summary of anomalies identified as part of a event ....” The examiner notes that “Cooper does not explicitly teach an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.”, and thus relies on Symantec. Specifically, the examiner argues: “A snooze for future alerts is taught Symantec though, such as in pages 4-9 and 5-6, wherein an event may be allowed to continue, and an alert may be prevented from appearing in the future.” The examiner also argues that: “One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user. Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity.”

Applicant contends that Symantec does not suggest all of the features of claim 1, namely, to snooze future alerts related to the event in the summary for a period of time. Symantec is directed to a virus protection program and not specifically to the claimed intrusion detection in a network. As understood, Symantec product is a machine based product and thus does not operate on network events. Thus, while Symantec does include a feature that allows an action to continue, “the remember control”, the remember control prevents the activity from appearing in the future and thus would not be useful in the context of Cooper, since it could permit what seems like innocuous events to be ignored and erroneously result in a serious network intrusion.

## Claim 2

Claim 2 further limits claim 1 to require that: “... the snooze control feature is selected based on event types and roles of hosts.” The examiner argues that: “... Symantec teaches wherein the snooze control feature can be selected based on event types (4-9 and 5-6, such as when events occur when copying

programs). Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158." Applicant contends that Cooper neither describes nor suggests that "the preventing of unnecessary alerts due to roles of hosts." Cooper at the cited passages have no such teaching of alerts based on grouping or roles of hosts. Symantec being directed to a stand-alone application would not be concerned with grouping or roles per se and therefore no combination of Cooper with Symantec would suggest the features of claim 2.

Claim 3 is allowable at least for analogous reasons as in claim 1.

#### Claim 4

Claim 4 limits claim 3 requiring that "an event details region of the graphical user interface depicts anomalies that were used to classify the event." The examiner argues that: "...Cooper teaches wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event (Figure 22)." Applicant disagrees. Cooper is not understood as dealing with anomalies (e.g., low level network discrepancies that are used to form and classify an event) and events. Therefore Cooper cannot teach that the "interface depicts anomalies that were used to classify the event."

Claims 5-9 are allowable at least because they depend directly or indirectly on claim 1. Independent claim 22 is allowable at least because of a similar rationale as argued for claim 1 and Claims 23 - 25 are allowable at least because they depend from claim 22.

The examiner rejected Claims 10-14 and 18 under 35 U.S.C. 103(a) as being unpatentable over Cooper and Symantec as applied above, and further in view of Billhartz US Patent No. 6,986,161 (hereinafter Billhartz).

Claim 10, as amended, calls for ... providing an operator with a list ... indicating event severity, with event severity ... having a percentage relationship to an established threshold ... providing on a graphical user interface a snooze control to allow a user to snooze future alerts related to the selected event.

Independent claim 10 is allowable, at least for the reasons argued in claim 1 above. In addition, the examiner notes that: However, Cooper and Symantec do not explicitly teach an event having a

percentage relationship to an established threshold for issuing an event notification. This is taught throughout Billhartz though, such as in col. 8 line 41 to col. 9 line 10.” Applicant disagrees. At the cited passage Billhartz is discussion collusions of network packets and a threshold based on collision rates to establish whether or not to raise an alert. However, Billhartz does not suggest “... event severity ... having a percentage relationship to an established threshold ... ,” as called for in the claim. Accordingly any combination of Cooper and Symantec with Billhartz does not suggest the claimed invention.

Claims 11, 13, 14, and 18 are allowable at least for the reasons discussed in claim 1.

Claim 12 is further distinct using the same basis of arguments as for claim 2 above.

The examiner rejected claims 15-17 and 21 under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Porras US Patent No. 6,321,338 (hereinafter Porras).

Claims 15-17 and 21 are allowable at least for the reasons discussed in claim 10.

The examiner rejected claim 19 under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Central Point's Central Point Anti-Virus- Virus detection, Removal and Prevention, 1991 (hereinafter Central Point).

Claim 19 is allowable at least for the reasons discussed in claim 10.

The examiner rejected claim 20 under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Kuroshita US Patent No. 5,550,807 (hereinafter Kuroshita).

Claims 20 is allowable at least for the reasons discussed in claim 10.

Enclosed is an Information Disclosure Statement. No combination of the art in the attached IDS nor the art of record describes or suggest the features of Applicant's claims.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

In view of the foregoing, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

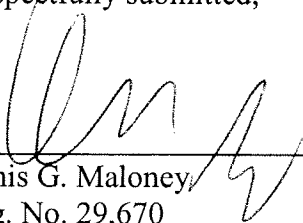
Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please charge the Petition for Extension of Time fee of **\$525** and please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: \_\_\_\_\_

12/1/07

  
\_\_\_\_\_  
Denis G. Maloney  
Reg. No. 29,670

Fish & Richardson P.C.  
225 Franklin Street  
Boston, MA 02110  
Telephone: (617) 542-5070  
Facsimile: (617) 542-8906